

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:
The premises known as the offices of
Google Inc., 1600 Amphitheatre
Parkway, Mountain View, CA 94043
Account: hungfun263@gmail.com

CR

19-MJ-14

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Elliott Harding, Detective with the Rapid City Police Department (RCPD) and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

1. I have been a law enforcement officer since December 1st of 2008. I have received training at the Law Enforcement Training Academy in Pierre, SD, training as a new police officer recruit along with various Police Training Officers and my own experience working in the Patrol Division. I have worked as a Detective in the Criminal Investigations Department beginning April of 2014 and primarily focused on stolen vehicles, pursuits and other general property crimes. During that time, I attended the Reid Technique of Interview and Interrogations. I have worked as a Detective in the Internet Crimes Against Children (ICAC) Task Force since August of 2015. During this time, I have attended classes in regards to on-line ads and undercover chat investigations as it pertains to child exploitation as well as prostitution/human trafficking. I have

also attended classes in regards to the BitTorrent Network as it pertains to the download and sharing of child pornography files. As a Special Assistant Attorney General with State of South Dakota my duties include investigations related to illegal possession and distribution of images containing sexually explicit material, and investigations dealing with illegal activities concerning the Internet or World Wide Web.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statues 18 U.S.C. §§ 2251, 2252 and 2252A, involving violations of law involving child pornography and 18 U.S.C. § 2422(b), enticement of a minor using the internet. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the manufacture, distribution, receipt, and possession of child pornography.

4. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of

documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a Google, Inc. account found during the investigation of an unknown subject utilizing the Target Account, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), and which items are more specifically described in Attachment B. The Gmail account is: hungfun263@gmail.com (also referred to in this affidavit as “Target Account”).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B:

a. “Chat,” as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat

messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Cloud-based storage service,” as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets,

anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. “Computer hardware,” as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form.

It commonly includes programs to run operating systems, applications, and utilities.

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

l. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

n. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

o. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

r. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

s. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY,
COMPUTERS, THE INTERNET, AND EMAIL**

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone.

These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

e. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail,

among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

8. Based on my training and experience and investigation in this case, I have learned the following about Google:

- a. Google offers an e-mail service that is available free to Internet users called "Gmail." Stored electronic communications, including opened and unopened e-mail for Gmail subscribers may be located on Google's computers.
- b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.
- c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.

d. When a user sends any e-mail to a Gmail e-mail subscriber the email is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, Google retains the email until the user deletes it or exceeds the storage limit.

f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e-mail.

9. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

10. On 11/26/18, I received CyberTip 42170700 from the National Center for Missing and Exploited Children. Google reported what they believed to be an image of child pornography. A copy of the Cybertip was copied to compact disc and stored in the ICAC lab. The following is a brief overview of information contained in this CyberTipline report:

Incident Type: Unconfirmed - Files not Reviewed by NCMEC

Please be advised that NCMEC staff have not opened or viewed any uploaded files submitted with this report and have no information concerning the content of the uploaded files other than information provided in the report by the ESP.

Total Uploaded Files: 1

11. I understand that Google identifies and reports child sexual abuse imagery in accordance with federal statutory definition of child pornography as referenced in 18 U.S.C. § 2256. Google has informed law enforcement of the following regarding Cybertips:

- a. If a report does not contain an upload IP, it may be because Google does not have the information accessible at the time of the report.
- b. To the extent that Google does have a record of the upload IP, it can be disclosed in response to valid legal process.
- c. Account information such as IP addresses and user provided information (such as SMS number or secondary e-mail address)

may change over time and/or reflect user provided data that may be inaccurate.

- d. As such, this information should be investigated and confirmed independently.
- e. Any account reported in a Cybertip may or may not be disabled in the course of making the report.
- f. With respect to the portion of this CyberTip containing the heading: "Was File Reviewed by Company?", when Google responds "Yes" it means the contents of the file reported were viewed by a person concurrently to or immediately preceding the sending of the CyberTip. When Google responds "No," it means that while the contents of the file were not reviewed concurrently to making the report, historically a person had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography.

12. Google's Cybertip also contained the following information:

- Incident Type: Child Pornography (possession, manufacture, and distribution)
- Incident Time: 10-22-2018 18:05:03 UTC; Description of Incident Time.
The incident date refers to the approximate date and time Google became aware of the reported material.
- Name: Nick Smith

- Email Address: hungfun263@gmail.com (Verified) (the SUBJECT ACCOUNT)
- IP Address: 24.111.56.83 (Registration) / 07-19-2015 01:28:33 UTC
 - *I would note that Maxmind showed the IP address 24.111.56.83 belonging to Midco, Location: Spearfish, SD.*
- Filename: Google-CT-RPT-454aa5c09e78a609212df64bda632510
- Original Filename Associated with File: 16863.jpeg
- Did Reporting ESP view entire contents of uploaded file? No
- Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
- Image Categorization by ESP: A1
 - *I am aware that Google defines A1 as a Prepubescent `Minor associated with a Sex Act (Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.)*

13. On 12/10/18, I sent a search warrant and affidavit, via email, to the Honorable Judge Chad Callahan regarding the CyberTip picture (Photo DNA) in question provided by Google, which as stated above, had not been previously viewed by anyone at Google.

14. On 12/10/18, I received the Photo DNA search warrant signed by the Honorable Judge Chad Callahan. Based on that warrant, I observed file Google-CT-RPT-454aa5c09e78a609212df64bda632510, which was in the Google Cybertip. The picture showed a female child between the ages of 3 and 5 years of age. The child appeared to have long blond hair and was wearing a pink shirt. The tip and part of the shaft of a nude, erect, adult penis was touching the child's mouth. The child's hand was touching the penis. The picture was taken close up and the child was looking into the camera. The identity of the male and child are unknown. The bottom right of the picture was printed "Kristin2000.spaces.ru." I searched for information on the image "Kristin2000.spaces.ru," and my ICAC computer redirected me to a website called spaces (spcs.me) which appeared to be a Russian website. I was unable to find anything directly related to Kristin or Kristin2000.

15. On 12/10/18, I sent a preservation letter to Google, via email, for email address hungfun263@gmail.com.

16. On 12/19/18, I received a Lawrence County subpoena for MidContinent Communications for IP address 24.111.56.83. I then sent the signed subpoena to MidContinent via email on 12/19/18. MidContinent replied stating they only keep recorded IP lease information for 18 months and did not have record of my request.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS
CHILD PORNOGRAPHY**

17. Based on my previous investigative experience related to child

exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs,

correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The user often maintains these child pornography images for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found within the SUBJECT ACCOUNT.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

18. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

19. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

20. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the following account: hungfun263@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Google, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Google, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

LIMIT ON SCOPE OF SEARCH

21. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

REQUEST FOR SEALING OF MATTER

22. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

CONCLUSION

23. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google, Inc. account, listed in Attachment A has been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Gmail account

received child pornography and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The account is: hungfun263@gmail.com.


24. Law Enforcement agents will serve the warrant on Google, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

25. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. via the internet and to allow Google, Inc. to copy the data outside of this agent's presence.

RETURN COMPLIANCE BY GOOGLE, INC.

26. Google's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Google requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

Dated: 1/16/19

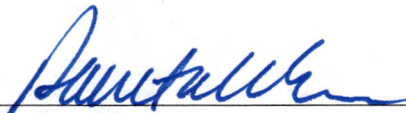

Detective Elliott Harding

Rapid City Police Department and ICAC

Sworn to before me and:

- ☒ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

this 16th day of January, 2019.


Daneta Wollmann

United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following Gmail email account, under an account known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043: hungfun263@gmail.com

ATTACHMENT B
**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

**I. Information to be disclosed by Google, Inc. (the “Provider”) to
facilitate execution of the warrant:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Google Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December 12, 2018. Google Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts’ user’s or owner’s true identity:

a. The contents of all e-mails associated with the account, from the time of the account’s creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account’s creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP addresses used to register the account, all log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of services utilized;

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Google Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, (production, receipt and possession of child pornography) including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

- a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;
- b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;
- c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;
- d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

- e. Evidence indicating the email account users or owner's state of mind as it relates to the crime under investigation;
- f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by Google:

Google shall disclose responsive data, if any, by sending to:

Detective Elliott Harding
Internet Crimes Against Children Taskforce
300 Kansas City Street, Suite 200
Rapid City, SD 57701
Elliott.Harding@rcgov.org
(605) 377-7420

Google shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, Google may make the responsive data available to Detective Harding by use of its law enforcement website.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is _____.

I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature